

软件

绝对可靠

勒索软件、木马、病毒：2017 年的 IT 世界受到了很高的威胁。企业怎样才能有效地防止网络攻击呢？物流软件供应商 AEB 公司给出了建议的方案，并为其他公司提供了安全保护的预防措施。



据 欧盟执法机构称，这是一场空前规模的网络攻击：勒索软件 WannaCry 在五月初就感染了全球 150 多个国家和地区的 230 000 多台计算机。这一勒索软件对计算机和网络上的文件进行加密，在支付赎金之后才能解密。遭受攻击时的情景是：联邦铁路的列车运行时刻表出现了故障信息，引起了轰动。许多工业企业和商业企业也受到了牵连。

数十亿的损失

几周之后，恶意程序 Petya 又开始传播了。受这一勒索木马感染的计算机将无法启动。这一恶意程序严重干扰了 TNT Express 公司的全球快递，也干扰了航运公司 Maersk 和德国邮政 DHL 的正常工作。

总而言之，网络威胁的风险正在增加。据 IT 行业协会 Bitkom 最近的一项研究显示，过去两年来，德国一半以上（53%）的企业成为工业间谍、恶意破坏或数据盗窃的受害者，每年带来的经济损失大约 550 亿欧元。与 2015 年度的调查研究相比较，增加了 6%。

防止侵害的八点计划

德国斯图加特市的软件供应商



图 1 计算中心有自己的规章制度。对此，AEB 建议：只使用当前的操作系统

AEB 公司负责 IT 技术的 Marting Setzler 先生努力克服当前遇到的种种威胁。这家企业是一家技术领先的物流和外贸软件供应商。“德国出口商很大一部分海关申报材料都是通过我们的数据中心完成的。客户对我们软件和服务非常放心。因此我们全面的 IT 安全防护方案是必不可少的。” Setzler 先生说。以下八点就是 AEB 公司整个 IT 安全防护系统的重点，也可以提供给其他企业支持它们的 IT 系统：

- 只使用当前的操作系统：过时的操作系统（例如 Windows XP, Vista 和 Windows 2003 等）都用当前的和升级版的系统所取代。
- 升级：在多级的自动升级过程中对所有服务器和客户端的程序都打好补丁。
- 多级备份：数据和整个服务器都定期的或者部分的在运行过程中备份，首先是备份到硬盘上，一段时间后备份到磁带上，并定期的保存在防火的



图 2 根据特定的标准在内部网络中对网络流量进行监控

另一个建筑物中。当然，这些数据都要经过加密处理。

- 下一代防火墙：网络流量也要根据特定的标准在内部网络中进行监控，并在必要时给予抑制。例如：这可以阻止客户端访问服务器的硬盘。或者阻止访客进入自己的网络中。这里的特定标准可以是任何标准，从地址到网络流中的特定模式。

- 查毒软件：AEB 在所有计算机中都安装了恶意软件扫描器。另外，在重要的‘神经节点’处，例如在邮件服务器那里辅助的采用了多层次的病毒扫描器。

- 自适应的危险防护和主动式线程防御：可执行文件在启动时都用本地的反恶意扫描软件进行扫描、分析。能够在毫秒级的时间段内从网络中查到该可执行文件的档案信誉，并阻止可疑文件的执行。未知的数据将自动的在封闭的环境进行分析（例如在‘沙箱’中），并在发现威胁时能够在几分钟内阻止其运行。

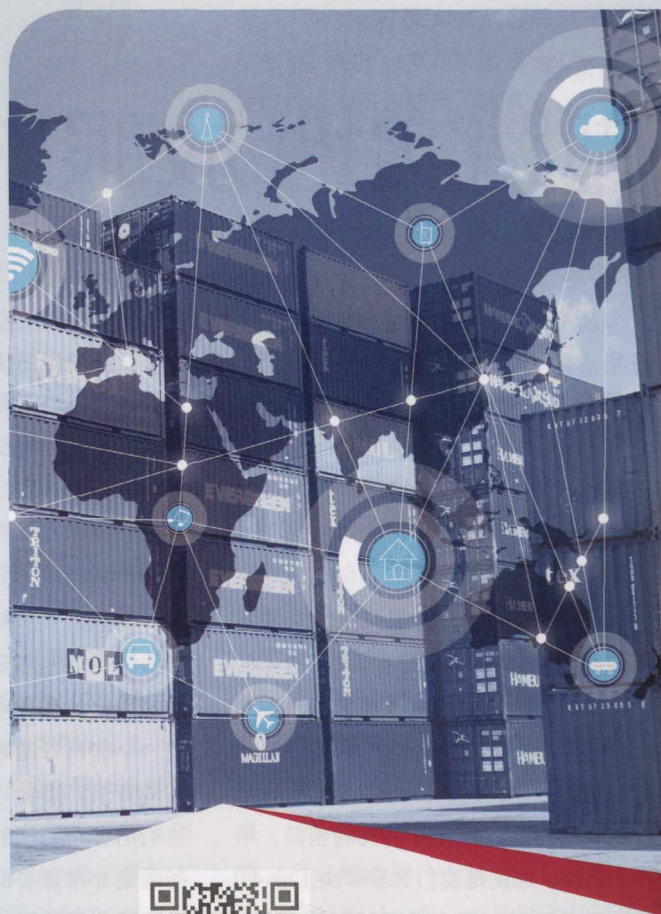
- 蜜罐技术：用一个单独的驱动器作为所有客户端恶意软件的诱饵也是非常有意义的。操作人员和确认的程序、文件是不会在这一驱动器上运行的。一旦这一驱动器的运行出现变化，大多数情况都是被恶意软件加密了。这时就会自动发出报警提示，也包括 SMS 报警：在最坏的情况下中央硬盘也会紧急关闭。

- 渗透测试：公司定期的请外部专家进行渗透测试，提高安全防范意识、避免损失。渗透测试后会知道企业网络中的薄弱环节，进行风险安全管理。MM

关注物流新动态 探讨物流新趋势!



现代物流



微信公众号

以“推动生产物流信息技术应用，促进物流信息资源整合”为核心，为物流行业中的管理者和技术工程师，提供物流技术、典型案例和成功经验等内容，搭建网上互动平台。



现代制造

联系我们：

电话 (Tel): +86-10-63326090-98

传真 (Fax): +86-10-63326099

E-mail: mm@vogel.com.cn



Vogel 弗戈工业传媒

MM 创刊于1894年

广告